ESET CYBER SECURITY PRO

per Mac

Manuale di installazione e Guida utente

Fare clic qui per scaricare la versione più recente di questo documento

ESET **CYBER SECURITY PRO**

Copyright © 2013 di ESET, spol. s r.o.
ESET Cyber Security Pro è stato sviluppato da ESET, spol. s r.o.
Per ulteriori informazioni visitare www.eset.it.
Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.
ESET, spol. s r.o. si riserva il diritto di modificare qualsiasi parte dell'applicazione software descritta senza alcun preavviso.

Supporto tecnico: http://www.nod32.it/support/index.php

REV. 11. 1. 2013

Contenuti

1. ESET Cyber Security Pro 4
1.1 Novità 4
1.2 Requisiti di sistema 4
2. Installazione 4
2.1 Installazione tipica 5
2.2 Installazione personalizzata 5
3. Attivazione del prodotto 6
4. Disinstallazione 6
5. Panoramica di base 6
5.1 Tasti di scelta rapida 6
5.2 Verifica del funzionamento del programma 7
5.3 Cosa fare se il programma non funziona correttamente 7
6. Protezione del computer 7
6.1 Protezione antivirus e antispyware 7
6.1.1 Protezione file system in tempo reale 7
6.1.1.1 Scansione al verificarsi di un evento 7
6.1.1.2 Opzioni avanzate 8
6.1.1.3 Quando modificare la configurazione della protezione in tempo reale 8
6.1.1.4 Controllo della protezione in tempo reale 8
6.1.1.5 Cosa fare se la protezione in tempo reale non funziona 8
6.1.2 Scansione del computer su richiesta 9
6.1.2.1 Tipo di scansione 9
6.1.2.1.1 Controllo Smart 9
6.1.2.1.2 Controllo personalizzato 9
6.1.2.2 Destinazioni di scansione 9
6.1.2.3 Profili di scansione 9
6.1.3 Esclusioni 10
6.1.4 Configurazione dei parametri del motore ThreatSense 10
6.1.4.1 Oggetti 10
6.1.4.2 Opzioni 11
6.1.4.3 Pulizia 11
6.1.4.4 Estensioni 11
6.1.4.5 Limiti 11
6.1.4.6 Altri 12
6.1.5 Rilevamento di un'infiltrazione 12
6.2 Controllo e blocco dei supporti rimovibili 13
7. Firewall 13
7.1 Modalità di filtraggio 13
7.2 Regole del firewall 13
7.2.1 Creazione di una nuova regola 14
7.3 Aree del firewall 14
7.4 Profili del firewall 14
7.5 Rapporti del firewall 14
8. Protezione Web ed e-mail 14
8.1 Protezione web 15
8.1.1 Porte 15
8.1.2 Modalità attiva 15
8.1.3 Elenchi URL 15
8.2 Protezione e-mail 15
8.2.1 Verifica del protocollo POP3 16
8.2.2 Verifica del protocollo IMAP 16
9. Parental control 16
10. Aggiornamento 16
10.1 Impostazione dell'aggiornamento 17
10.2 Come creare attività di aggiornamento 17
10.3 Upgrade di ESET Cyber Security Pro ad una nuova versione 17
11. Strumenti 17
11.1 File di registro 18
11.1.1 Manutenzione registro 18
11.1.2 Filtraggio registri 18
11.2 Pianificazione attività 18
11.2.1 Creazione di nuove attività 19
11.2.2 Creazione di un'attività definita dall'utente 19
11.3 Quarantena 19
11.3.1 Mettere file in quarantena 20
11.3.2 Ripristino dalla quarantena 20
11.3.3 Invio di file dalla Quarantena 20
11.4 Processi in esecuzione 20
11.5 Live Grid 20
11.5.1 Configurazione Live Grid 21
12. Interfaccia utente 21
12.1 Avvisi e notifiche 21
12.1.1 Configurazione avanzata avvisi e notifiche 21
12.2 Privilegi 22
12.3 Menu contestuale 22
13. Varie 22
13.1 Importa ed esporta impostazioni 22
13.1.1 Importa impostazioni 22
13.1.2 Esporta impostazioni 22
13.2 Configurazione del server proxy 22
14. Glossario 23
14.1 Tipi di infiltrazioni 23
14.1.1 Virus 23
14.1.2 Worm 23
14.1.3 Trojan horse 23
14.1.4 Rootkit 24
14.1.5 Adware 24
14.1.6 Spyware 24
14.1.7 Applicazioni potenzialmente pericolose 24
14.1.8 Applicazioni potenzialmente indesiderate 25
14.2 Tipi di attacchi remoti 25
14.2.1 Attacchi DoS 25
14.2.2 DNS Poisoning 25
14.2.3 Attacchi worm 25
14.2.4 Controllo delle porte 25
14.2.5 Desincronizzazione del TCP 25
14.2.6 SMB Relay 25
14.2.7 Attacchi ICMP 26
14.3 E-mail 26
14.3.1 Pubblicità 26
14.3.2 Hoax 26
14.3.3 Phishing 27
14.3.4 Riconoscimento di messaggi spam 27

1. ESET Cyber Security Pro

ESET Cyber Security Pro rappresenta un nuovo approccio ad una sicurezza realmente integrata. La versione più recente del motore di controllo ThreatSense®, combinata con la protezione del client di posta, il Personal firewall e il Parental control, sfrutta velocità e precisione per garantire la sicurezza del computer. Il risultato è un sistema intelligente costantemente in allerta contro gli attacchi e i software dannosi che possono compromettere il computer.

ESET Cyber Security Pro è il risultato di sforzi a lungo termine per una soluzione di sicurezza completa in grado di combinare la massima protezione con un impatto minimo sul sistema. Le tecnologie avanzate basate sull'intelligenza artificiale sono in grado di eliminare in modo proattivo l'infiltrazione di virus, worm, trojan horse, spyware, adware, rootkit e altri attacchi trasportati da Internet senza rallentare le prestazioni del sistema o interrompere l'attività del computer.

1.1 Novità

Firewall
Il Personal firewall consente di controllare tutto il traffico di rete da e verso il sistema. Tale operazione è possibile accettando o rifiutando le singole connessioni di rete basate su specifiche regole di filtraggio. Il sistema offre protezione contro gli attacchi provenienti da computer remoti e attiva il blocco di alcuni servizi.

Parental control
L'opzione del Parental control consente di bloccare i siti che potrebbero contenere materiale potenzialmente offensivo. I genitori possono impedire l'accesso ad un massimo di 27 categorie predefinite di siti web. Questo strumento consentirà di impedire a bambini e ragazzi di avere accesso a pagine con contenuti inadeguati o pericolosi.

Protezione client di posta
La protezione e-mail garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP.

Controllo supporti rimovibili
ESET Cyber Security Pro offre un controllo su richiesta del dispositivo multimediale rimovibile inserito (CD, DVD, USB, dispositivo iOS e così via).

Unitevi alla rete ESET Live Grid
Costruito sul sistema avanzato di allarme immediato ThreatSense.NET, ESET Live Grid è stato concepito allo scopo di offrire livelli di sicurezza aggiuntivi ai computer degli utenti. Tale sistema consente di monitorare costantemente i programmi e i processi in esecuzione sul sistema grazie alle più recenti informazioni raccolte da milioni di utenti ESET in tutto il mondo. Inoltre, poiché le dimensioni del database ESET Live Grid aumentano col tempo, i controlli di sistema vengono eseguiti in modo più rapido e più preciso. Ciò consente di offrire a tutti gli utenti una protezione proattiva più ampia e una migliore velocità di controllo. Vi consigliamo di attivare questa funzione e vi ringraziamo per il vostro sostegno.

Nuovo design
La finestra principale di ESET Cyber Security Pro è stata completamente riprogettata e, nella nuova versione, le impostazioni avanzate (Preferenze) sono più intuitive e garantiscono una navigazione più semplice.

1.2 Requisiti di sistema

Per un funzionamento ottimale di ESET Cyber Security Pro, il sistema deve soddisfare i seguenti requisiti hardware e software:

	Requisiti di sistema
Architettura processore	32 bit, 64 bit Intel®
Sistema operativo	Mac OS X 10.6 e successivo
Memoria	300 MB
Spazio libero su disco	150 MB

2. Installazione

Prima di cominciare la procedura di installazione, chiudere tutti i programmi aperti sul computer. In ESET Cyber Security Pro sono contenuti componenti che possono creare conflitto con altri programmi antivirus già installati nel computer. ESET accomanda vivamente di rimuovere eventuali altri programmi antivirus per evitare potenziali problemi.

Per avviare la procedura guidata di installazione, procedere in uno dei modi descritti di seguito:

- Se si utilizza il CD/DVD di installazione, inserirlo nel computer, aprirlo dal Desktop o dalla finestra **Finder** e fare doppio clic sull'icona **Installa**.
- Se si utilizza un file scaricato dal sito Web ESET, aprirlo e fare doppio clic sull'icona **Installa**.

Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi di configurazione di base. Durante la fase iniziale dell'installazione, il programma di installazione ricercherà automaticamente l'ultima versione del prodotto on-line. Se l'ultima versione del prodotto viene trovata, il programma di installazione la metterà a disposizione per il download e avvierà il processo di installazione.

Dopo aver accettato i termini dell'accordo di licenza dell'utente finale, è possibile scegliere una delle seguenti modalità di installazione:

- Installazione tipica 5
- Installazione personalizzata 5

2.1 Installazione tipica

La modalità installazione tipica comprende le opzioni di configurazione adatte alla maggior parte degli utenti. Queste impostazioni garantiscono livelli massimi di sicurezza, nonché prestazioni ottimali del sistema. L'installazione tipica rappresenta l'opzione predefinita consigliata nel caso in cui gli utenti non abbiano particolari necessità relative a impostazioni specifiche.

Live Grid
Il Sistema di allarme immediato Live Grid è uno strumento in grado di informare in modo immediato e costante ESET sulle nuove infiltrazioni allo scopo di garantire una protezione rapida ai clienti. Il sistema consente di inviare le nuove minacce al Laboratorio ESET, dove queste vengono analizzate, elaborate e aggiunte nel database delle firme antivirali. Per impostazione predefinita, viene selezionata l'opzione **Attiva Sistema di allarme immediato Live Grid**. Fare clic su **Configura...** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, consultare la sezione Live Grid 20.

Applicazioni speciali
Il passaggio finale del processo di installazione consiste nella configurazione del rilevamento delle **Applicazioni potenzialmente indesiderate**. Tali programmi non sono necessariamente dannosi. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile rilevarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Dopo aver installato ESET Cyber Security Pro, sarà necessario eseguire un controllo del computer per ricercare eventuali codici dannosi. Nella finestra principale del programma, fare clic su **Scansione computer**, quindi fare clic su **Scansione intelligente**. Per ulteriori informazioni sulle scansioni del computer su richiesta, si rimanda alla sezione Controllo del computer su richiesta 9.

2.2 Installazione personalizzata

La modalità di installazione personalizzata è indicata per utenti esperti che desiderano modificare le impostazioni avanzate durante il processo di installazione.

Server proxy
In caso di utilizzo di un server proxy, è possibile definirne i parametri durante questa fase selezionando l'opzione **Utilizzo un server proxy**. Nella fase successiva, immettere l'indirizzo IP o URL del server proxy nel campo **Indirizzo**. Nel campo **Porta**, specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario immettere un **Nome utente** e una **Password** validi per consentire l'accesso al server proxy. Se si è certi di non utilizzare un server proxy, scegliere l'opzione **Non utilizzo un server proxy**. In caso di dubbi, è possibile utilizzare le impostazioni di sistema correnti selezionando **Utilizza le impostazioni di sistema (scelta consigliata)**.

Privilegi
Nel passaggio successivo, è possibile definire gli utenti con privilegi che saranno in grado di modificare la configurazione del programma. Dalla lista di utenti sulla sinistra, è possibile scegliere gli utenti e l'opzione **Aggiungi** alla lista degli **Utenti con privilegi**. Per visualizzare tutti gli utenti del sistema, selezionare l'opzione **Mostra tutti gli utenti**. Se la lista di Utenti con privilegi viene lasciata vuota, tutti gli utenti saranno considerati utenti con privilegi.

Live Grid
Il Sistema di allarme immediato Live Grid è uno strumento in grado di informare in modo immediato e costante ESET sulle nuove infiltrazioni allo scopo di garantire una protezione rapida ai clienti. Il sistema consente di inviare le nuove minacce al Laboratorio ESET, dove queste vengono analizzate, elaborate e aggiunte nel database delle firme antivirali. Per impostazione predefinita, viene selezionata l'opzione **Attiva Sistema di allarme immediato Live Grid**. Fare clic su **Configura...** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, consultare la sezione Live Grid 20.

Applicazioni speciali
Il passaggio successivo del processo di installazione consiste nella configurazione del rilevamento delle **Applicazioni potenzialmente indesiderate**. Tali programmi non sono necessariamente dannosi. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile rilevarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Personal Firewall: modalità di filtraggio
Nel passaggio finale, è possibile selezionare una modalità di filtraggio per il Personal Firewall. Per ulteriori informazioni, vedere Modalità di filtraggio 13.

Dopo aver installato ESET Cyber Security Pro, sarà necessario eseguire un controllo del computer per ricercare eventuali codici dannosi. Nella finestra principale del programma, fare clic su **Scansione computer**, quindi fare clic su **Scansione intelligente**. Per ulteriori informazioni sulle scansioni del computer su richiesta, si rimanda alla sezione Scansione del computer su richiesta 9.

3. Attivazione del prodotto

Dopo l'installazione, sullo schermo comparirà automaticamente la finestra **Tipo di attivazione del prodotto**. In alternativa, è possibile fare clic sull'icona ESET Cyber Security Pro collocata sulla barra dei menu (parte superiore della schermata) quindi su **Attivazione del prodotto...**.

1. Se il prodotto è stato acquistato presso un rivenditore, selezionare l'opzione **Attivazione tramite chiave** . La chiave di attivazione è generalmente collocata all'interno o sul retro della confezione del prodotto. Per una corretta attivazione, è necessario inserire la chiave fornita.

2. Se sono stati ricevuti un nome utente e una password, selezionare l'opzione **Attivazione tramite nome utente e password** e inserire i dati di licenza negli appositi campi. Questa opzione equivale all'opzione **Configurazione nome utente e password...** nella finestra **Aggiornamento** del programma.

3. Se si desidera provare ESET Cyber Security Pro prima di acquistarlo, selezionare l'opzione **Attiva licenza di prova**. Inserire l'indirizzo e-mail per attivare ESET Cyber Security Pro per un periodo limitato. La licenza di prova verrà inviata all'indirizzo e-mail fornito. È possibile attivare una sola licenza di prova per cliente.

Se si sceglie di non attivare la licenza in questo momento, fare clic su **Attiva In seguito**. È possibile attivare ESET Cyber Security Pro direttamente dalla sezione **Stato protezione** o **Aggiorna** della finestra principale del programma ESET Cyber Security Pro.

Se non si dispone di una licenza e si desidera acquistarne una, fare clic sull'opzione **Licenza**. In tal modo, si verrà reindirizzati al sito Web o al distributore locale ESET.

4. Disinstallazione

Se si desidera disinstallare ESET Cyber Security Pro dal computer, procedere in uno dei modi descritti di seguito:

- inserire il CD/DVD di installazione ESET Cyber Security Pro nel computer, aprirlo dal desktop o dalla finestra **Finder** e fare doppio clic sull'icona **Disinstalla**,
- aprire il file di installazione ESET Cyber Security Pro (*.dmg*) e fare doppio clic sull'icona **Disinstalla**,
- lanciare il **Finder**, aprire la cartella **Applicazioni** sul disco rigido, premere ctrl e fare clic sull'icona **ESET Cyber Security Pro**, quindi selezionare l'opzione **Mostra contenuti pacchetto**. Aprire la cartella **Risorse** e fare doppio clic sull'icona **Disinstallazione**.

5. Panoramica di base

La finestra principale di ESET Cyber Security Pro è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

- **Stato protezione** - fornisce informazioni relative allo stato di protezione del computer, del firewall, del Web e delle e-mail, nonché del Parental control.
- **Controllo computer** - questa opzione consente di configurare e avviare il Controllo del computer su richiesta 9.
- **Aggiorna** - consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.
- **Configurazione** - selezionare questa opzione per regolare il livello di sicurezza del computer.
- **Strumenti** - consente di accedere ai File di rapporto 18, alla Pianificazione attività 18, alla Quarantena 19, ai Processi in esecuzione 20 e ad altre funzionalità del programma.
- **Guida** - consente di visualizzare l'accesso ai file della guida, alla Knowledge base su Internet, al modulo di richiesta di assistenza al Supporto tecnico e ad altre informazioni sul programma.

5.1 Tasti di scelta rapida

I tasti di scelta rapida disponibili durante l'utilizzo di ESET Cyber Security Pro sono:

- *cmd-,* - consente di visualizzare le Preferenze ESET Cyber Security Pro,
- *cmd-U* - consente di aprire la finestra **Configurazione nome utente e password**,
- *cmd-alt-T* - consente di aprire la finestra **Caratteri speciali**,
- *cmd-O* - consente di ridimensionare la finestra principale dell'interfaccia grafica utente (GUI) di ESET Cyber Security Pro impostando le dimensioni predefinite e di spostarla al centro della schermata,
- *cmd-alt-H* - consente di nascondere tutte le finestre aperte ad eccezione di ESET Cyber Security Pro,
- *cmd-H* - consente di nascondere ESET Cyber Security Pro.

I seguenti tasti di scelta rapida funzionano solo se viene attivata l'opzione **Utilizza menu standard** in **Configurazione** > **Inserisci preferenze applicazione...** (oppure premere *cmd-,*) > **Interfaccia**:

- *cmd-alt-L* - consente di aprire la sezione **File di rapporto**,
- *cmd-alt-S* - consente di aprire la sezione **Pianificazione attività**,
- *cmd-alt-Q* - consente di aprire la sezione **Quarantena**.

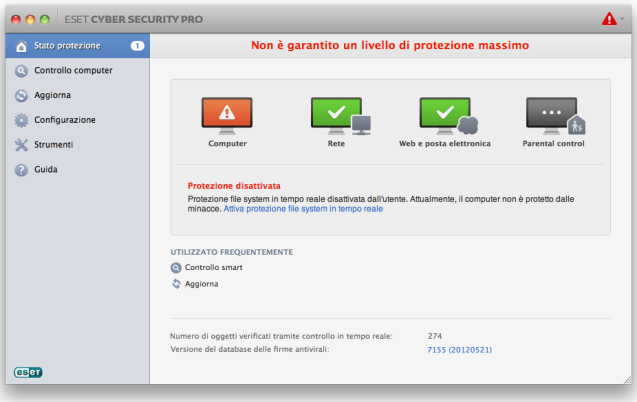
5.2 Verifica del funzionamento del programma

Per visualizzare lo stato di protezione, fare clic sull'opzione **Stato protezione** dal menu principale. Nella finestra principale verrà visualizzato un rapporto di funzionamento dei moduli ESET Cyber Security Pro.

5.3 Cosa fare se il programma non funziona correttamente

Se i moduli attivati funzionano correttamente, verrà visualizzata un'icona verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione. Verranno visualizzate ulteriori informazioni sul modulo e una soluzione consigliata del problema. Per modificare lo stato di ciascun modulo, fare clic sul collegamento blu sotto ciascun messaggio di notifica.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, è possibile condurre una ricerca nella Knowledge base ESET oppure contattare il Supporto tecnico ESET, che risponderà prontamente alle domande degli utenti fornendo assistenza nella risoluzione del problema.


ESET CYBER SECURITY PRO
Stato protezione
Controllo computer
Aggiorna
Configurazione
Strumenti
Guida
Non è garantito un livello di protezione massimo
Computer
Rete
Web e posta elettronica
Parental control
Protezione disattivata
Protezione file system in tempo reale disattivata dall'utente. Attualmente, il computer non è protetto dalle minacce. Attiva protezione file system in tempo reale
UTILIZZATO FREQUENTEMENTE
Controllo smart
Aggiorna
Numero di oggetti verificati tramite controllo in tempo reale: 274
Versione del database delle firme antivirali: 7155 (20120521)

6. Protezione del computer

È possibile trovare la configurazione del computer nella sezione **Configurazione** > **Computer**, in cui viene visualizzato lo stato della **Protezione file system in tempo reale** e del **Blocco dei supporti rimovibili**. Per disattivare i singoli moduli, impostare il pulsante del modulo desiderato sullo stato **DISATTIVATO**. Nota: tale operazione potrebbe limitare la protezione del computer. Per accedere alle impostazioni dettagliate di ciascun modulo, fare clic sul pulsante **Configurazione...**.

6.1 Protezione antivirus e antispyware

La protezione antivirus difende il sistema da attacchi dannosi, modificando i file che rappresentano minacce potenziali. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla bloccandola e pulendola, eliminandola o mettendola in quarantena.

6.1.1 Protezione file system in tempo reale

La protezione file system in tempo reale controlla tutti i tipi di supporto e attiva una scansione quando si verificano determinati eventi. Mediante l'utilizzo dei metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione intitolata Configurazione dei parametri del motore ThreatSense 10), la protezione file system in tempo reale potrebbe essere diversa per i file appena creati o quelli esistenti. Nel caso di file appena creati, è possibile applicare un livello di controllo maggiore.

In base alle impostazioni predefinite, la protezione in tempo reale viene attivata automaticamente all'avvio del sistema operativo e fornisce un controllo ininterrotto. In casi speciali, ad esempio in caso di conflitto con un altro scanner in tempo reale, la protezione in tempo reale può essere interrotta facendo clic sull'icona ESET Cyber Security Pro collocata sulla barra dei menu (sulla parte superiore dello schermo) e selezionando quindi l'opzione **Disattiva la protezione file system in tempo reale**. La protezione in tempo reale può essere interrotta anche dalla finestra principale del programma (fare clic su **Configurazione** > **Computer** e impostare la **Protezione file system in tempo reale** sullo stato **DISATTIVATA**).

Per modificare le impostazioni avanzate della protezione in tempo reale, fare clic su **Configurazione** > **Inserisci preferenze applicazione ...** (oppure premere *cmd-,*) > **Protezione in tempo reale** e fare clic sul pulsante **Configurazione...** vicino a **Opzioni avanzate** (descritte nella sezione intitolata Opzioni avanzate di controllo 8).

6.1.1.1 Scansione al verificarsi di un evento

Per impostazione predefinita, il controllo viene effettuato all'apertura dei file, durante la creazione dei file o l'esecuzione dei file. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

6.1.1.2 Opzioni avanzate

In questa finestra è possibile definire le tipologie di oggetti da sottoporre a controllo da parte del motore ThreatSense e attivare/disattivare l'opzione **Euristica avanzata**, nonché modificare le impostazioni degli archivi e della cache file.

Si consiglia di non modificare i valori predefiniti nella sezione **Impostazioni predefinite archivi** salvo nel caso in cui fosse necessario risolvere un problema specifico, poiché livelli di ricerca degli archivi troppo elevati possono ostacolare le prestazioni del sistema.

È possibile passare al controllo euristico avanzato ThreatSense per i file eseguiti, creati e modificati separatamente facendo clic sulla casella di controllo **Euristica avanzata** nelle rispettive sezioni dei parametri ThreatSense.

Al fine di determinare un impatto minimo sul sistema durante l'utilizzo della protezione in tempo reale, è possibile definire le dimensioni della cache di ottimizzazione. Tale comportamento è attivo nel momento in cui si sceglie l'opzione **Attiva pulisci cache file**. Quando questa funzione è disattivata, tutti i file vengono controllati a ogni accesso. I file non verranno sottoposti a scansione ripetutamente dopo essere stati memorizzati nella cache (salvo il caso in cui siano stati modificati) fino alle dimensioni definite della cache. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali. Fare clic su **Attiva pulisci cache file** per attivare/disattivare questa funzione. Per impostare il numero di file da memorizzare nella cache, basta indicare il valore desiderato nel campo di inserimento accanto alla voce **Dimensioni cache**.

È possibile impostare ulteriori parametri di controllo nella finestra **Configurazione motore ThreatSense**. È possibile definire il tipo di **Oggetti** da sottoporre a scansione, le **Opzioni** da utilizzare e il livello di **Pulizia**, nonché definire le **Estensioni** e i **Limiti** delle dimensioni dei file per la protezione file system in tempo reale. È possibile accedere alla finestra di configurazione del motore ThreatSense facendo clic sul pulsante **Configurazione...** vicino a **Motore ThreatSense** nella finestra Configurazione avanzata. Per ulteriori informazioni relative ai parametri del motore ThreatSense, si rimanda alla sezione Configurazione dei parametri del motore ThreatSense 10.

6.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Agire con prudenza nel momento in cui si modificano i parametri della protezione in tempo reale. È consigliabile modificarli solo in casi specifici, come ad esempio il caso in cui si verifichi un conflitto con una determinata applicazione o con lo scanner in tempo reale di un altro programma antivirus.

Dopo l'installazione di ESET Cyber Security Pro, tutte le impostazioni sono ottimizzate al fine di offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Impostazioni predefinite** posizionato nell'angolo in basso a sinistra della finestra **Protezione in tempo reale** (**Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione in tempo reale**).

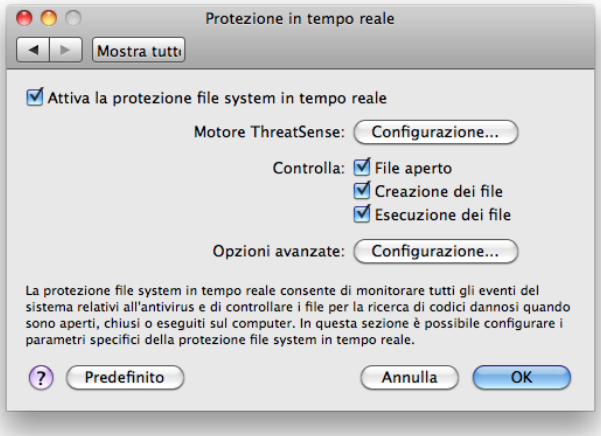
6.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare il file di test eicar.com. Questo file di test è un file innocuo, speciale, rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus.

6.1.1.5 Cosa fare se la protezione in tempo reale non funziona

Nel prossimo capitolo verranno illustrate situazioni problematiche che si possono verificare quando si utilizza la protezione in tempo reale e verranno descritte le relative modalità di risoluzione.

La protezione in tempo reale è disattivata
Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, accedere a **Configurazione** > **Computer** e impostare la **Protezione file system in tempo reale** sullo stato **ATTIVATA**. In alternativa, è possibile attivare la protezione file system in tempo reale nella finestra preferenze applicazione in **Protezione in tempo reale** selezionando l'opzione **Attiva protezione file system in tempo reale**.


Protezione in tempo reale
Mostra tutti
Attiva la protezione file system in tempo reale
Motore ThreatSense:
Configurazione...
Controlla:
File aperto
Creazione dei file
Esecuzione dei file
Opzioni avanzate:
Configurazione...
La protezione file system in tempo reale consente di monitorare tutti gli eventi del sistema relativi all'antivirus e di controllare i file per la ricerca di codici dannosi quando sono aperti, chiusi o eseguiti sul computer. In questa sezione è possibile configurare i parametri specifici della protezione file system in tempo reale.
Predefinito
Annulla
OK

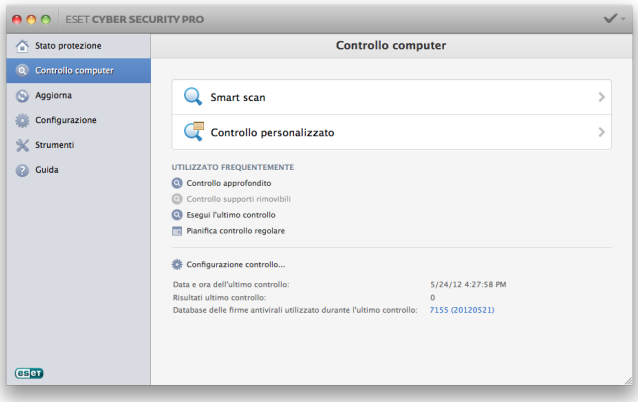
La protezione in tempo reale non rileva né pulisce le infiltrazioni
Assicurarsi che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, essi possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus che potrebbero essere presenti nel sistema.

La protezione in tempo reale non viene avviata
Se la protezione in tempo reale non si attiva all'avvio del sistema, ciò potrebbe dipendere da conflitti con altri programmi. In questo caso, consultare gli specialisti del Supporto tecnico ESET.

6.1.2 Scansione del computer su richiesta

Se si sospetta che il computer sia infetto perché non funziona normalmente, eseguire una **Scansione computer** > **Scansione intelligente** per cercare eventuali infiltrazioni nel computer. Per garantire un livello massimo di protezione, è necessario eseguire regolarmente controlli del computer come parte delle misure di sicurezza di routine, anziché limitarsi ad eseguirle in caso di infezioni sospette. Una scansione regolare consente di rilevare infiltrazioni non rilevate dallo scanner in tempo reale se salvate su disco. Ciò accade se, al momento dell'infezione, lo scanner in tempo reale è stato disattivato o quando il database di firme antivirali è obsoleto.

È consigliabile eseguire una scansione del computer su richiesta almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**.



È inoltre possibile trascinare i file e le cartelle selezionati dal Desktop o dalla finestra **Finder** sulla schermata principale di ESET Cyber Security Pro, sull'icona del dock, sull'icona sulla barra dei menu (parte superiore della schermata) o sull'icona dell'applicazione (collocata nella cartella */ Applicazioni*).

6.1.2.1 Tipo di scansione

Sono disponibili due tipologie di scansione del computer su richiesta. **Scansione intelligente**, che consente di eseguire rapidamente la scansione del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente di selezionare uno dei profili di controllo predefiniti, nonché di scegliere destinazioni di controllo specifiche.

6.1.2.1.1 Controllo Smart

La funzione controllo Smart consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio principale è la semplicità della procedura, che non richiede una configurazione di scansione dettagliata. Il controllo Smart consente di effettuare un controllo di tutti i file presenti nelle cartelle, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di disinfezione viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulizia, si rimanda alla sezione dedicata alla Pulizia 11.

6.1.2.1.2 Controllo personalizzato

Il **Controllo personalizzato** rappresenta una soluzione ottimale se si desidera specificare parametri di scansione quali destinazioni e metodi di scansione. Il vantaggio del controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare diverse configurazioni come profili di scansione definiti dagli utenti. Questi sono particolarmente utili se la scansione viene eseguita più volte con gli stessi parametri.

Per scegliere le destinazioni di scansione, selezionare **Controllo computer** > **Controllo personalizzato** quindi selezionare **Destinazioni di scansione** specifiche dalla struttura ad albero. Una destinazione di scansione può anche essere specificata in modo più preciso, immettendo il percorso alla cartella dei file che si desidera includere nel controllo. Se si desidera controllare solo il sistema senza ulteriori azioni di pulizia, selezionare l'opzione **Scansione senza rimozione**. È inoltre possibile scegliere tra tre livelli di disinfezione selezionando **Configurazione...** > **Pulizia**.

NOTA: L'esecuzione di scansioni del computer attraverso il controllo personalizzato è un'operazione raccomandata per gli utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

6.1.2.2 Destinazioni di scansione

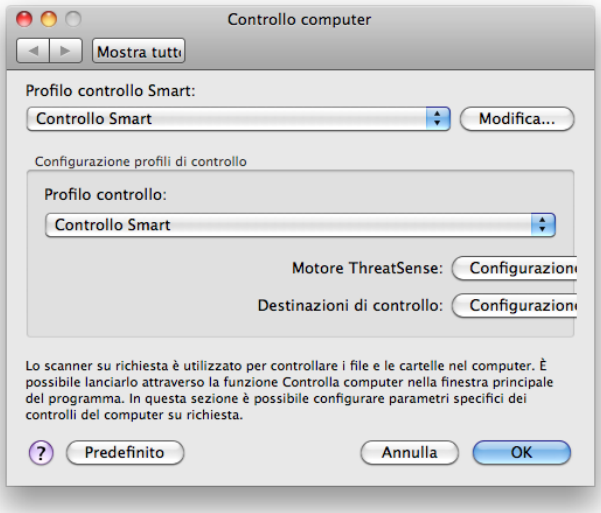
La struttura ad albero delle destinazioni di scansione consente di selezionare i file e le cartelle da sottoporre a scansione anti-virus. È altresì possibile selezionare le cartelle in base alle impostazioni di un determinato profilo.

Una destinazione di scansione può essere definita in modo più preciso, immettendo il percorso alla cartella dei file che si desidera includere nel controllo. Selezionare le destinazioni dalla struttura ad albero contenente una lista di tutte le cartelle presenti nel computer.

6.1.2.3 Profili di scansione

È possibile salvare le impostazioni di scansione preferite per scansioni future. È consigliabile creare un profilo di scansione differente (con diverse destinazioni di scansione, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, accedere alla sezione **Configurazione** > **Inserisci preferenze applicazione ...** (oppure premere *cmd-,*) > **Controllo computer** e fare clic su **Modifica...** vicino alla lista dei profili correnti.


Controllo computer
Mostra tutt
Profilo controllo Smart:
Controllo Smart
Modifica...
Configurazione profili di controllo
Profilo controllo:
Controllo Smart
Motore ThreatSense:
Configurazion
Destinazioni di controllo:
Configurazion
Lo scanner su richiesta è utilizzato per controllare i file e le cartelle nel computer. È possibile lanciarlo attraverso la funzione Controlla computer nella finestra principale del programma. In questa sezione è possibile configurare parametri specifici dei controlli del computer su richiesta.
Predefinito
Annulla
OK

Per ricevere assistenza nella creazione di un profilo di controllo adatto alle proprie esigenze, si rimanda alla sezione Configurazione dei parametri del motore ThreatSense 10 contenente una descrizione di ciascun parametro di configurazione del controllo.

Esempio: Si supponga di voler creare il proprio profilo di scansione e che la configurazione della Scansione intelligente sia appropriata solo in parte, in quanto non si desidera eseguire la scansione di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione di Massima pulizia. Nella finestra **Lista profili scanner su richiesta**, digitare il nome del profilo, fare clic sul pulsante **Aggiungi** e confermare facendo clic su **OK**. Specificare quindi i parametri in base alle proprie esigenze impostando **Motore ThreatSense** e **Destinazioni di controllo**.

6.1.3 Esclusioni

La sezione (**Configurazione** > **Inserire preferenze applicazione...** > **Esclusioni**) consente di escludere alcuni file/ cartelle, applicazioni o indirizzi IP/IPv6 dal controllo.

I file e le cartelle presenti nell'elenco **FileSystem** saranno esclusi da tutti i controlli: sistema (avvio), in tempo reale e su richiesta.

- **Percorso** - percorso dei file e delle cartelle esclusi
- **Minaccia** - se è presente il nome di una minaccia accanto a un file escluso, significa che il file viene escluso solo per la minaccia indicata e non per tutte. Pertanto, se il file si infetta successivamente con altri malware, esso verrà rilevato dal modulo antivirus.
- **Aggiungi...**- esclude gli oggetti dal rilevamento. Inserire il percorso a un oggetto (è anche possibile utilizzare i caratteri jolly * e ?) o selezionare la cartella o il file dalla struttura ad albero.
- **Modifica...** - consente di modificare le voci selezionate
- **Elimina** - rimuove le voci selezionate
- **Impostazioni predefinite** - annulla tutte le esclusioni.

Nella scheda **Web ed e-mail**, è possibile escludere alcune **Applicazioni** o alcuni **Indirizzi IP/IPv6** dal controllo del protocollo.

6.1.4 Configurazione dei parametri del motore ThreatSense

ThreatSense è la tecnologia proprietaria di ESET costituita da una serie di complessi metodi di rilevamento delle minacce. Questa tecnologia è proattiva, il che significa che fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Essa utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare notevolmente la protezione del sistema. Il motore di controllo è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione della tecnologia ThreatSense consentono all'utente di specificare diversi parametri di controllo:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per accedere alla finestra di configurazione, fare clic su **Configurazione > Inserire preferenze applicazione...** (oppure premere *cmd-,*), quindi fare clic sul pulsante del motore ThreatSense **Configurazione...** collocato nei caratteri jolly **Protezione sistema**, **Protezione in tempo reale** e **Controllo computer**, che utilizzano la tecnologia ThreatSense (vedere la sezione sottostante). Scenari di protezione diversi possono richiedere configurazioni diverse. Ciò detto, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- **Protezione sistema** - Controllo automatico file di avvio
- **Protezione file system in tempo reale** - Protezione file system in tempo reale
- **Controllo computer** - Controllo del computer su richiesta.

I parametri ThreatSense sono ottimizzati in modo specifico per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica delle impostazioni per il controllo degli eseguibili compressi o per consentire il controllo euristico avanzato nel modulo di protezione del file system in tempo reale potrebbe provocare un rallentamento del sistema. È quindi consigliabile non modificare i parametri predefiniti ThreatSense per tutti i moduli, con l'eccezione di Controllo computer.

6.1.4.1 Oggetti

Nella sezione **Oggetti** è possibile definire i file del computer che saranno sottoposti a controllo per la ricerca di infiltrazioni.

- **File** - consente di eseguire il controllo di tutti i tipi di file più comuni (programmi, immagini, file audio, file video, database e così via).

- **Collegamenti simbolici** - (solo per controllo su richiesta): consentono di effettuare il controllo di tipologie speciali di file contenenti una stringa di testo interpretata e seguita dal sistema operativo come percorso ad un altro file o ad un'altra directory.
- **File di e-mail** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare il controllo di file speciali contenenti messaggi di posta elettronica.
- **Caselle di posta** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare il controllo delle caselle di posta del sistema. Un uso scorretto di questa opzione potrebbe determinare un conflitto con il client di posta. Per ulteriori informazioni relative ai vantaggi e agli svantaggi di tale opzione, consultare il seguente articolo relativo alla knowledge base.
- **Archivi** - (non disponibile nel caso della protezione in tempo reale) consente di eseguire il controllo dei file compressi in archivi (.rar, .zip, .arj, .tar e così via).
- **Archivi autoestraenti** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare il controllo dei file contenuti in file di archivi autoestraenti.
- **Eseguibili compressi** - a differenza dei file di archivio standard, i file eseguibili compressi vengono decompressi in memoria, in aggiunta agli eseguibili statici standard (UPX, yoda, ASPack, FGS e così via).

6.1.4.2 Opzioni

Nella sezione **Opzioni**, è possibile selezionare i metodi utilizzati durante un controllo del sistema per il rilevamento di eventuali infiltrazioni. Sono disponibili le seguenti opzioni:

- **Euristica** - L'euristica è un algoritmo che analizza le attività (dannose) dei programmi. Il vantaggio principale del rilevamento euristico consiste nella possibilità di rilevare un nuovo software dannoso che in precedenza non esisteva o che non era incluso nell'elenco dei virus conosciuti (database di firme antivirali).
- **Euristica avanzata** - L'euristica avanzata comprende un algoritmo di euristica unico, sviluppato da ESET, ottimizzato per il rilevamento di worm e trojan horse scritto in linguaggi di programmazione di alto livello. Grazie all'euristica avanzata, la capacità di rilevamento del programma è decisamente più elevata.
- **Applicazioni potenzialmente indesiderate** - Si tratta di applicazioni non necessariamente dannose. Tuttavia, esse potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. I cambiamenti più significativi comprendono finestre popup indesiderate, attivazione ed esecuzione di processi nascosti, aumento dell'utilizzo delle risorse di sistema, modifiche dei risultati delle ricerche e applicazioni che comunicano con server remoti.
- **Applicazioni potenzialmente pericolose** - tali applicazioni si riferiscono a software commerciali e legali che possono essere sfruttati dagli aggressori informatici se installati all'insaputa dell'utente. Tale classificazione comprende programmi quali strumenti di accesso remoto. Pertanto, questa opzione è disattivata per impostazione predefinita.

6.1.4.3 Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia:

- **Nessuna pulizia** - I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione.
- **Pulizia standard** - Il programma tenterà di pulire o di eliminare automaticamente un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma proporrà una serie di azioni di follow-up. La scelta tra queste azioni verrà visualizzata anche nel caso in cui non possa essere completata un'azione predefinita.
- **Massima pulizia** - Il programma pulirà o eliminerà tutti i file infetti (inclusi gli archivi). Le uniche eccezioni sono rappresentate dai file di sistema. Nel caso in cui non fosse possibile pulire tali file, l'utente potrà intraprendere un'azione all'interno di una finestra di avviso.

Attenzione: nella modalità Pulizia standard, viene eliminato l'intero file di archivio solo se tutti i file contenuti sono infetti. Nel caso in cui fossero presenti anche file non infetti, esso non verrà eliminato. Se nella modalità Massima pulizia viene rilevato un file di archivio infetto, verrà eliminato l'intero archivio, anche se sono presenti file puliti.

6.1.4.4 Estensioni

Un'estensione è la parte di nome del file delimitata da un punto. L'estensione definisce il tipo e il contenuto del file. Questa sezione della configurazione dei parametri ThreatSense consente di definire i tipi di file da escludere dal controllo.

Per impostazione predefinita, tutti i file vengono sottoposti a controllo indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dal controllo. I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire il controllo delle estensioni desiderate.

L'esclusione di file dal controllo è talvolta utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento del programma. Ad esempio, è consigliabile escludere le estensioni *.log*, *.cfg* e *.tmp*.

6.1.4.5 Limiti

La sezione **Limiti** consente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire il controllo:

- **Dimensioni massime:** Consente di definire la dimensione massima degli oggetti da sottoporre a controllo. Il modulo antivirus eseguirà unicamente il controllo degli oggetti di dimensioni inferiori a quelle specificate. Si consiglia di non modificare il valore predefinito, poiché di norma non sussiste alcun motivo per farlo. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dal controllo.

- **Durata massima controllo:** Consente di definire il valore massimo di tempo destinato al controllo di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà il controllo di un oggetto una volta raggiunto tale valore temporale, indipendentemente dal fatto che il controllo sia stato completato.
- **Livello massimo di nidificazione:** Consente di specificare il livello massimo di controllo degli archivi. Si consiglia di non modificare il valore predefinito di 10; in circostanze normali, non sussiste alcun motivo per farlo. Se il controllo termina prima del tempo a causa del numero di archivi nidificati, l'archivio non verrà controllato.
- **Dimensioni massime file:** Questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi da sottoporre a controllo una volta estratti. Se, a causa di tale limite, il controllo termina prima del tempo, l'archivio non verrà controllato.

6.1.4.6 Altri

Attiva ottimizzazione Smart
L'attivazione dell'ottimizzazione Smart consente di ottimizzare le impostazioni allo scopo di garantire il miglior livello di controllo, senza comprometterne la velocità. I vari moduli di protezione eseguono il controllo in modo intelligente, utilizzando metodi di controllo differenti. L'ottimizzazione Smart non è definita in modo rigido all'interno del prodotto. Il team di sviluppo ESET provvede costantemente all'implementazione di nuove modifiche che vengono successivamente integrate in ESET Cyber Security Pro attraverso aggiornamenti regolari. Se l'opzione ottimizzazione Smart non è attivata, durante il controllo vengono applicate solo le impostazioni definite dall'utente di moduli specifici nell'architettura ThreatSense.

Controlla flussi dati alternativi (Solo per controllo su richiesta) Flussi di dati alternativi (fork risorsa/dati) utilizzati dal file system, sono associazioni di file e cartelle invisibili alle tecniche di controllo standard. Numerose infiltrazioni tentano di non essere rilevate presentandosi come flussi di dati alternativi.

6.1.5 Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi accessi: pagine web, cartelle condivise, messaggi e-mail o periferiche rimovibili (USB, dischi esterni, CD, DVD e così via).

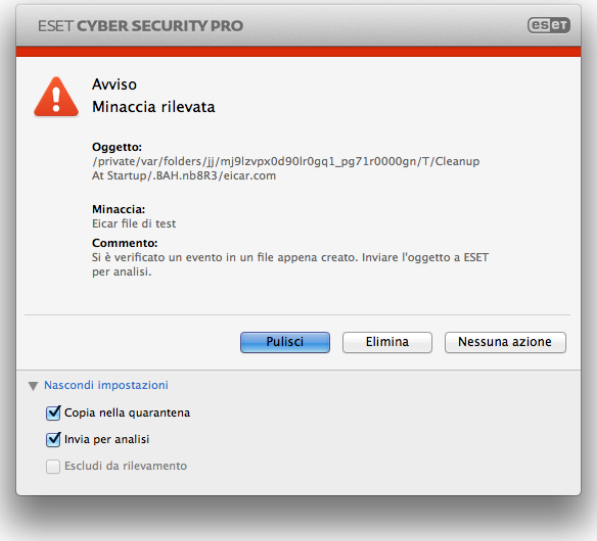
Se il computer mostra segnali di infezione da malware (ad esempio appare più lento, si blocca spesso e così via), è consigliabile seguire le seguenti istruzioni:

1. Fare clic su **Controllo computer**.
2. Fare clic su **Controllo Smart** (per ulteriori informazioni, vedere la sezione Controllo Smart 9).
3. Al termine della scansione, controllare nel registro il numero di file sottoposti a scansione, di file infetti e di file puliti.

Se si desidera effettuare la scansione solo di una parte del disco, scegliere **Scansione personalizzata** e selezionare gli oggetti da controllare alla ricerca di virus.

Per avere un'idea generale di come ESET Cyber Security Pro gestisce le infiltrazioni, si supponga che il monitoraggio del file system in tempo reale, che utilizza il livello di pulizia predefinito, rilevi un'infiltrazione. Verrà eseguito il tentativo di pulire o eliminare il file. In assenza di azioni predefinite disponibili per il modulo di protezione in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, poiché con tale opzione si lasciano i file infetti inalterati. È opportuno selezionare questa opzione solo quando si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.

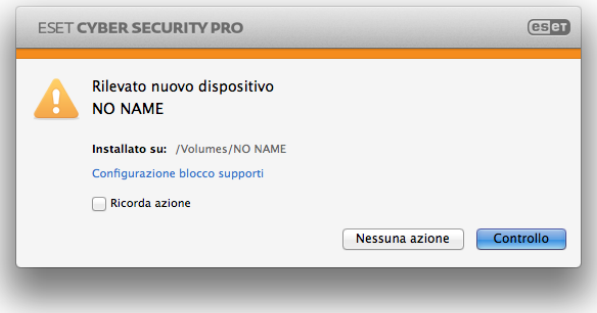
Pulizia ed eliminazione - Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto al file pulito un codice dannoso. In tal caso, tentare in primo luogo di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codici dannosi, verrà eliminato.



Eliminazione dei file negli archivi - In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. È tuttavia consigliabile essere prudenti durante l'esecuzione di una scansione di **Massima pulizia**, poiché in questa modalità l'archivio viene eliminato anche se contiene un solo file infetto, indipendentemente dallo stato degli altri file dell'archivio.

6.2 Controllo e blocco dei supporti rimovibili

ESET Cyber Security Pro offre un controllo su richiesta del dispositivo multimediale rimovibile inserito (CD, DVD, USB, dispositivo iOS e così via).



I supporti rimovibili potrebbero contenere codici dannosi e mettere a rischio il computer. Per bloccare i supporti rimovibili, fare clic su **Configurazione blocco supporti** (vedere l'immagine in alto) o **Configurazione** > **Inserire preferenze applicazione...** > **Supporti** dalla finestra principale del programma e selezionare l'opzione **Attiva blocco supporti rimovibili**. Per consentire l'accesso a talune tipologie di supporti multimediali, deselezionare i volumi dei supporti desiderati.

NOTA: se si desidera consentire l'accesso all'unità CD-ROM esterna collegata al computer mediante il cavo USB, deselezionare l'opzione **CD-ROM**.

7. Firewall

Il Personal firewall consente di controllare tutto il traffico di rete da e verso il sistema. Tale operazione è possibile accettando o rifiutando le singole connessioni di rete basate su specifiche regole di filtraggio. Il sistema offre protezione contro gli attacchi provenienti da computer remoti e attiva il blocco di alcuni servizi. Il Personal firewall offre anche protezione antivirus per i protocolli HTTP, POP3 e IMAP. Questa funzionalità rappresenta un elemento molto importante per la sicurezza del computer.

È possibile trovare la configurazione del Personal firewall nella sezione **Configurazione** > **Firewall**. Ciò consente di regolare la modalità, le regole e le impostazioni dettagliate di filtraggio. Da qui, è inoltre possibile accedere a impostazioni più dettagliate del programma.

Impostando l'opzione **Blocca tutto il traffico di rete: disconnetti rete** sullo stato **ATTIVATA**, tutte le comunicazioni in entrata e in uscita verranno bloccate dal Personal firewall. Utilizzare questa opzione solo se si sospettano rischi di sicurezza critici che richiedono la disconnessione del sistema dalla rete.

7.1 Modalità di filtraggio

Sono disponibili tre modalità di filtraggio per ESET Cyber Security Pro Personal firewall. È possibile trovare le modalità di filtraggio nelle preferenze ESET Cyber Security Pro (premere *cmd-,*) > **Firewall**. Il comportamento del firewall cambia in base alla modalità selezionata. Le modalità di filtraggio influenzano inoltre il livello richiesto di interazione dell'utente.

Tutto il traffico bloccato - tutte le connessioni in entrata e in uscita verranno bloccate.

Automatico con eccezioni - modalità predefinita. Questa modalità è adatta agli utenti che preferiscono un utilizzo semplice e comodo del firewall, senza dover definire delle regole. La modalità automatica consente il traffico standard in uscita per il sistema e blocca tutte le connessioni non inizializzate avviate sul lato rete. È anche possibile aggiungere regole personalizzate e definite dall'utente.

Modalità interattiva - consente di creare una configurazione personalizzata per il Personal firewall. Quando viene rilevata una comunicazione e non esiste alcuna regola applicabile, viene visualizzata una finestra di dialogo che segnala una connessione sconosciuta. La finestra di dialogo consente di accettare o rifiutare la comunicazione e la decisione può essere ricordata come nuova regola del Personal firewall. Se l'utente decide di creare una nuova regola, tutte le connessioni future di questo tipo saranno consentite o bloccate in base a questa regola.

Per ulteriori informazioni relative a tutte le connessioni bloccate in un file di rapporto, selezionare l'opzione **Registra tutte le connessioni bloccate**. Per accedere ai file di rapporto del firewall, fare clic su **Strumenti** > **Rapporti**, quindi selezionare **Firewall** dal menu a discesa **Rapporto**.

7.2 Regole del firewall

Le regole rappresentano un insieme di condizioni utilizzate per verificare tutte le connessioni di rete e tutte le azioni assegnate a queste condizioni. Nel caso in cui sia stabilita una connessione definita da una regola, nel Personal firewall è possibile stabilire l'azione da eseguire.

Le connessioni in entrata vengono avviate da un computer

remoto che tenta di stabilire una connessione con il sistema locale. Le connessioni in uscita funzionano in senso opposto: il sistema locale tenta di stabilire la connessione con un computer remoto.

Quando viene rilevata una nuova comunicazione sconosciuta, è necessario considerare con attenzione se accettarla o rifiutarla. Le connessioni non desiderate, non sicure o sconosciute costituiscono un rischio per la protezione del sistema. Se si stabilisce una connessione di questo tipo, è opportuno prestare particolare attenzione al computer remoto e all'applicazione che tenta di connettersi al computer. Molte infiltrazioni cercano di ottenere e inviare dati privati o scaricare altre applicazioni dannose sulle workstation host. Il Personal firewall consente di rilevare e interrompere queste connessioni.

7.2.1 Creazione di una nuova regola

La scheda **Regole** contiene un elenco di tutte le regole applicate al traffico generato dalle singole applicazioni. Le regole vengono aggiunte automaticamente in base alle reazioni dell'utente ad una nuova comunicazione.

Per creare una nuova regola, fare clic sul pulsante **Aggiungi...**, inserire un nome per la regola e trascinare l'icona dell'applicazione nel riquadro bianco oppure fare clic su **Sfoglia...** per ricercare il programma nella cartella */ Applicazioni*. Se si desidera applicare la regola a tutte le applicazioni installate sul computer, selezionare l'opzione **Tutte le applicazioni**.

Nel passaggio successivo, specificare l'**Azione** (accettare o negare la comunicazione tra l'applicazione selezionata e la rete) e la **Direzione** della comunicazione (in entrata, in uscita o entrambe). Se si desidera registrare tutte le comunicazioni correlate a questa regola in un file di rapporto, selezionare l'opzione **Registra regola**. Per accedere ai rapporti, fare clic su **Strumenti** > **Rapporti**, dal menu principale ESET Cyber Security Pro, quindi selezionare **Firewall** dal menu a discesa **Rapporto**.

Nella sezione **Protocollo/Porte**, selezionare un protocollo mediante il quale l'applicazione comunica e i numeri delle porte (se si seleziona il protocollo TCP o UDP). Il livello del protocollo di trasmissione offre un trasferimento di dati sicuro ed efficiente.

L'ultimo passaggio consiste nello specificare la destinazione (indirizzo IP, intervallo, subnet, Ethernet o Internet).

7.3 Aree del firewall

Le aree rappresentano una serie di indirizzi di rete che creano un gruppo logico unico. A ciascun indirizzo del gruppo specificato vengono assegnate regole simili, definite in modo centralizzato per l'intero gruppo.

È possibile creare queste aree facendo clic sul pulsante **Aggiungi...**. Inserire un **Nome** e una **Descrizione** (facoltativo) dell'area, scegliere un profilo di appartenenza di quest'area e aggiungere un indirizzo IPv4/IPv6, un intervallo di indirizzi, una subnet, una rete WiFi o un'interfaccia.

7.4 Profili del firewall

L'opzione **Profili** consente di controllare il comportamento di ESET Cyber Security Pro Personal firewall. Durante la creazione o la modifica di una regola di Personal firewall, è possibile assegnarla ad un profilo specifico o applicarla a ciascun profilo. Se si seleziona un profilo, vengono applicate solo le regole globali (senza alcun profilo specificato) e le regole che sono state assegnate a quel profilo. Per modificare in modo semplice il comportamento del Personal firewall, è possibile creare più profili con varie regole assegnate.

7.5 Rapporti del firewall

Il Personal firewall ESET Cyber Security Pro salva tutti gli eventi importanti in un file di rapporto, che è possibile visualizzare direttamente dal menu principale. Fare clic su **Strumenti** > **Rapporti**, quindi selezionare **Firewall** dal menu a discesa **Rapporto**.

I file di rapporto rappresentano uno strumento prezioso per il rilevamento degli errori e delle intrusioni nel sistema. I rapporti di ESET Personal firewall contengono i dati che seguono:

- Data e ora dell'evento
- Nome dell'evento
- Fonte
- Indirizzo di rete di destinazione
- Protocollo di comunicazione di rete
- Regola applicata oppure nome dell'eventuale worm identificato
- Applicazione coinvolta
- Utente

Un'analisi approfondita di questi dati consente di rilevare i tentativi di compromissione della sicurezza del sistema. Numerosi altri fattori indicano indicano rischi di sicurezza potenziali e consentono all'utente di ridurne l'impatto: connessioni troppo frequenti da reti sconosciute, numerosi tentativi di creazione di connessioni, comunicazioni tra applicazioni sconosciute oppure utilizzo di numeri di porte insoliti.

8. Protezione Web ed e-mail

La configurazione della protezione Web ed e-mail è presente nella sezione **Configurazione** > **Web ed e-mail**. Da qui, è anche possibile accedere alle impostazioni dettagliate di ciascun modulo.

Protezione accesso Web e antiphishing - se attivata (scelta consigliata), la protezione file system in tempo reale monitora costantemente tutti gli eventi relativi all'antivirus.

Protezione client di posta - garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP.

8.1 Protezione web

La protezione dell'accesso al web consiste nel controllo della comunicazione dei web browser con server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol).

8.1.1 Porte

Nella scheda **Porte**, è possibile definire i numeri delle porte utilizzate per la comunicazione HTTP. I numeri delle porte predefiniti sono 80, 8080 e 3128.

8.1.2 Modalità attiva

ESET Cyber Security Pro prevede anche il sottomenu **Modalità attiva**, che definisce la modalità di controllo per i web browser. La modalità attiva consente di esaminare i dati trasferiti dalle applicazioni che hanno accesso a Internet in generale, indipendentemente dal fatto che siano contrassegnati o meno come web browser. Se questa opzione non è attivata, le comunicazioni provenienti dalle applicazioni vengono monitorate gradualmente in batch. Ciò riduce l'efficacia del processo di verifica dei dati, ma offre al contempo una maggiore compatibilità per le applicazioni elencate. Se non ci sono problemi di utilizzo, si consiglia di attivare la modalità di verifica attiva selezionando la casella di controllo vicino all'applicazione desiderata.

Quando un'applicazione controllata scarica i dati, questi vengono salvati dapprima in un file temporaneo creato da ESET Cyber Security Pro. I dati non sono disponibili per la specifica applicazione in quel momento. Una volta completato il download, i dati vengono controllati per la ricerca di codice dannoso. Se non vi sono infiltrazioni, i dati vengono inviati all'applicazione originale. Questo processo offre un controllo completo delle comunicazioni effettuate da un'applicazione controllata. Se viene attivata la modalità passiva, i dati vengono inviati in modo graduale all'applicazione originale per evitare timeout.

8.1.3 Elenchi URL

La sezione **Elenchi URL** consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo. I siti web contenuti nell'elenco di indirizzi bloccati non saranno accessibili. I siti web contenuti nell'elenco di indirizzi esclusi sono accessibili senza dover essere controllati per la ricerca di codice dannoso.

Se si desidera consentire l'accesso solo agli indirizzi URL presenti nell'elenco **URL consentito**, selezionare l'opzione **Limita indirizzi URL**.

Per attivare un elenco, selezionare l'opzione **Attivato**. Se si desidera ricevere una notifica relativa all'inserimento di un indirizzo proveniente dall'elenco corrente, selezionare l'opzione **Notificato**.

In tutti gli elenchi, è possibile utilizzare i simboli speciali * (asterisco) e *?* (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri e il punto interrogativo sostituisce qualsiasi simbolo. È necessario prestare particolare attenzione quando si specificano gli indirizzi esclusi, in quanto l'elenco dovrebbe contenere esclusivamente indirizzi affidabili e sicuri. Allo stesso modo, è necessario assicurarsi che i simboli * e ? vengano utilizzati correttamente in questo elenco.

8.2 Protezione e-mail

La protezione e-mail garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Durante il controllo dei messaggi in arrivo, il programma utilizza i metodi di controllo avanzato forniti dal motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi avviene ancora prima del confronto con il database delle firme antivirali. Il controllo delle comunicazioni mediante i protocolli POP3 e IMAP è indipendente dal client di posta utilizzato.

Motore ThreatSense - la configurazione avanzata dello scanner virus consente di configurare le destinazioni di controllo, i metodi di rilevamento e così via. Fare clic su **Configurazione...** per visualizzare la finestra delle impostazioni dettagliate dello scanner.

Dopo che un'e-mail è stata controllata, potrebbe essere aggiunta al messaggio una notifica contenente il risultato del controllo. È possibile selezionare l'opzione **Aggiungi notifiche all'oggetto di un'e-mail**. Poiché potrebbero essere omesse in messaggi HTML problematici oppure create da alcuni virus, non è possibile creare notifiche che non contengono una domanda. Sono disponibili le seguenti opzioni:

Mai - non verrà aggiunta alcuna notifica,
Solo per l'e-mail infetta - verranno contrassegnati come controllati solo i messaggi contenenti un software dannoso,
Per tutte le e-mail controllate - il programma aggiungerà messaggi a tutte le e-mail controllate.

Modello aggiunto all'oggetto di un'e-mail infetta - modificare questo modello se si desidera modificare il formato del prefisso dell'oggetto di un'e-mail infetta.

Aggiungi notifica alla nota a piè di pagina di un'e-mail - selezionare questa casella di controllo se si desidera che la protezione e-mail aggiunga un allarme virus all'e-mail infetta. Questa funzione consente di eseguire un semplice filtraggio delle e-mail infette e di aumentare il livello di credibilità del destinatario. Inoltre, in caso di rilevamento di un'infiltrazione, essa fornisce informazioni preziose relative al livello di minaccia di un'e-mail o di un mittente specifici.

8.2.1 Verifica del protocollo POP3

Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client di posta. ESET Cyber Security Pro offre protezione per questo protocollo, indipendentemente dal client di posta utilizzato.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato. Il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono controllate tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

Se l'opzione **Attiva verifica protocollo POP3** è attivata, viene monitorato tutto il traffico che ha luogo mediante il protocollo POP3 per la ricerca di software dannosi.

8.2.2 Verifica del protocollo IMAP

Il protocollo di accesso ai messaggi Internet (IMAP) è un altro protocollo Internet per il recupero delle e-mail. Il protocollo IMAP presenta alcuni vantaggi rispetto al protocollo POP3, tra cui la possibilità di connessione simultanea di più client alla stessa casella di posta e di conservazione delle informazioni sullo stato dei messaggi, come ad esempio il fatto che il messaggio sia stato letto o meno, abbia ricevuto risposta o sia stato eliminato. ESET Cyber Security Pro offre protezione per questo protocollo, indipendentemente dal client di posta utilizzato.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Per un corretto funzionamento del modulo, assicurarsi che sia attivato. Il controllo del protocollo IMAP viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono controllate tutte le comunicazioni della porta 143, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

Se l'opzione **Attiva verifica protocollo IMAP** è attivata, viene monitorato tutto il traffico che ha luogo mediante il protocollo IMAP per la ricerca di software dannosi.

9. Parental control

La sezione **Parental control** consente di configurare le impostazioni del parental control che offre ai genitori strumenti automatici per la protezione dei propri figli. L'obiettivo consiste nell'impedire a bambini e ragazzi di avere acceso a pagine con contenuti inadeguati o pericolosi. Il Parental control consente di bloccare le pagine web che potrebbero contenere materiale potenzialmente offensivo. I genitori possono anche impedire l'accesso ad un massimo di 27 categorie predefinite di siti web.

Gli account utenti sono elencati nella finestra **Parental Control** (**Configurazione** > **Inserire preferenze applicazione...** > **Parental Control**). Selezionare l'opzione che si desidera utilizzare per il parental control. Per specificare un livello di protezione per l'account selezionato, fare clic sul pulsante **Configurazione...**. Se si desidera creare un nuovo account, fare clic sul pulsante **Aggiungi...**. Tale operazione reindirizzerà l'utente alla finestra degli account del sistema operativo Mac.

Nella finestra **Configurazione Parental control**, selezionare uno dei profili predefiniti dal menu a discesa **Configura profilo** oppure copiare la configurazione del parental control da un altro account utente. Ciascun profilo contiene l'elenco modificato delle categorie consentite. Se una categoria è selezionata, ciò significa che è consentita. Spostando il mouse su una categoria, verrà visualizzato un elenco di pagine web che rientrano in quella categoria.

Se si desidera modificare l'elenco delle **Pagine web consentite e bloccate**, fare clic sul pulsante **Configurazione...** nella parte inferiore della finestra e aggiungere il nome di un dominio nell'elenco desiderato. Non digitare *http://*. L'utilizzo di caratteri jolly (*) non è necessario. Se si digita solo il nome di un dominio, verranno inclusi tutti i sottodomini. Ad esempio, se si aggiunge *google.com* nell'**Elenco delle pagine web consentite**, tutti i sottodomini (*mail.google.com*, *news.google.com*, *maps.google.com* e così via) saranno consentiti.

NOTA: il blocco o l'accettazione di una specifica pagina web può essere più accurato del blocco o dell'accettazione di un'intera categoria di pagine web.

10. Aggiornamento

Per garantire il massimo livello di sicurezza, è necessario aggiornare regolarmente ESET Cyber Security Pro. Il modulo di aggiornamento garantisce l'aggiornamento costante del programma grazie alla possibilità di scaricare il database delle firme antivirali più recente.

Facendo clic su **Aggiorna** nel menu principale, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente e valutare se sia necessario un aggiornamento. Per avviare manualmente il processo di aggiornamento, fare clic su **Aggiorna database delle firme antivirali**.

In circostanze normali, quando gli aggiornamenti sono scaricati correttamente, viene visualizzato il messaggio **Il database delle firme antivirali è aggiornato** nella finestra Aggiornamento. Se non è possibile aggiornare il database delle firme antivirali, si raccomanda di verificare le impostazioni di aggiornamento 17 - la causa più frequente per questo errore è l'immissione errata di dati di autenticazione (Nome utente e Password) o la configurazione errata delle impostazioni di connessione 22.

La finestra di aggiornamento contiene anche informazioni relative alla versione del database di firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito web ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

NOTA: il nome utente e la password vengono forniti da ESET dopo l'acquisto di ESET Cyber Security Pro.

10.1 Impostazione dell'aggiornamento

L'autenticazione per il server di aggiornamento si basa sul Nome utente e sulla Password generati e inviati dopo l'acquisto del programma.

Per attivare l'utilizzo della modalità test (download degli aggiornamenti pre-rilascio), fare clic sul pulsante **Configurazione** > **Inserire preferenze applicazione...** (oppure premere *cmd-,*) > **Aggiornamento**, fare clic sul pulsante **Configurazione...** vicino a **Opzioni avanzate** e selezionare la casella di controllo **Attiva aggiornamenti pre-rilascio**.

Per disattivare la visualizzazione delle notifiche sulla barra delle applicazioni al completamento dell'aggiornamento eseguito con successo, selezionare la casella di controllo **Non visualizzare notifiche relative agli aggiornamenti avvenuti con successo**.

Per eliminare tutti i dati di aggiornamento archiviati temporaneamente, fare clic sul pulsante **Cancella** accanto a **Cancella cache aggiornamento**. Utilizzare questa opzione in caso di problemi relativi all'aggiornamento.

10.2 Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente, selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale.

Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET Cyber Security Pro sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna di queste attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, vedere la sezione Pianificazione attività 18.

10.3 Upgrade di ESET Cyber Security Pro ad una nuova versione

Per assicurare la massima protezione, è importante utilizzare la build più recente di ESET Cyber Security Pro. Per verificare la disponibilità di una nuova versione, fare clic su **Stato protezione** dal menu principale sulla sinistra. Verrà visualizzato un messaggio in caso di disponibilità di una nuova build. Fare clic su **Per saperne di più...** per visualizzare una nuova finestra contenente il numero di versione della nuova build e il ChangeLog.

Fare clic su **Sì** per scaricare l'ultima build oppure su **Non ora** per chiudere la finestra e scaricare l'upgrade in un secondo momento.

Se si seleziona **Sì**, il file verrà scaricato nella cartella Download (oppure nella cartella predefinita impostata dal browser in uso). Al termine del download, avviare il file e attenersi alle istruzioni di installazione. Il nome utente e la password verranno trasferiti automaticamente alla nuova installazione. Si consiglia di verificare periodicamente la disponibilità degli aggiornamenti, soprattutto quando si esegue l'installazione di ESET Cyber Security Pro dal CD o dal DVD.

11. Strumenti

Il menu **Strumenti** contiene dei moduli che semplificano l'amministrazione del programma e offrono opzioni aggiuntive agli utenti avanzati.

11.1 File di registro

I file di registro contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta uno strumento essenziale per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di registro correnti. È possibile visualizzare i messaggi di testo e i registri direttamente dall'ambiente di ESET Cyber Security Pro, nonché dai registri di archivio.

È possibile accedere ai file di rapporto dal menu principale ESET Cyber Security Pro facendo clic su **Strumenti** > **Rapporti**. Selezionare il tipo di registro desiderato dal menu a discesa **Registro** nella parte superiore della finestra. Sono disponibili i registri seguenti:

1. **Minacce rilevate** - scegliere questa opzione per visualizzare tutte le informazioni sugli eventi relativi al rilevamento delle infiltrazioni.
2. **Eventi** - questa opzione è utile agli amministratori del sistema e agli utenti per la risoluzione dei problemi. Tutte le azioni importanti eseguite da ESET Cyber Security Pro vengono registrate nei registri degli eventi.
3. **Controllo computer** - in questa finestra vengono visualizzati i risultati di tutti i controlli completati. Fare doppio clic su una voce per visualizzare i dettagli della rispettiva scansione del computer su richiesta.
4. **Parental** - elenco di tutte le pagine web bloccate dal Parental control.
5. **Firewall** - risultati di tutti gli eventi correlati alla rete.

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti, selezionando la voce desiderata e facendo clic sul pulsante **Copia**.

11.1.1 Manutenzione registro

La configurazione della registrazione di ESET Cyber Security Pro è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Inserisci preferenze applicazione ...** (oppure premere *cmd-,*) > **File di rapporto**. Per i file di registro è possibile specificare le opzioni seguenti:

- **Elimina automaticamente i file di registro** - le voci del registro con data precedente al numero di giorni specificato vengono automaticamente eliminate.
- **Ottimizza automaticamente i file di registro** - i file di registro vengono automaticamente deframmentati se viene superata la percentuale specificata di record inutilizzati

Per configurare il **Filtro predefinito dei record di registro** fare clic sul pulsante **Modifica...** e selezionare/deselezionare i tipi di registro come richiesto.

11.1.2 Filtraggio registri

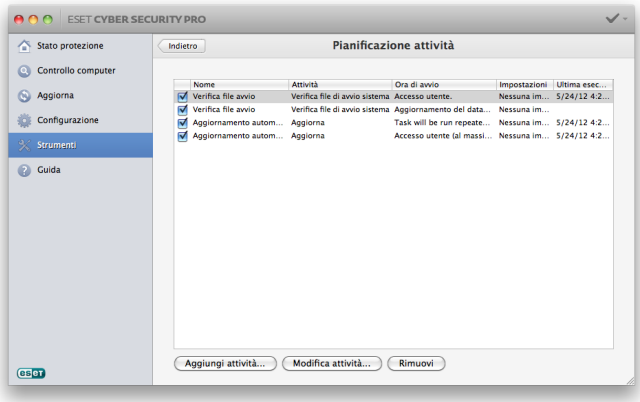
I registri memorizzano le informazioni relative a eventi importanti di sistema. La funzione di filtraggio del registro consente di visualizzare i record di un determinato tipo di evento.

I tipi di registro utilizzati più spesso sono elencati di seguito:

- **Allarmi critici** - errori critici di sistema (es. Impossibile avviare la protezione antivirus)
- **Errori** - messaggi di errore come "*Errore durante il download del file*" ed errori critici
- **Allarmi** - messaggi di allarme
- **Record informativi**- messaggi informativi che includono gli aggiornamenti riusciti, gli avvisi e così via.
- **Record diagnostici** - informazioni necessarie per la sincronizzazione ottimale del programma nonché di tutti i record riportati sopra.

11.2 Pianificazione attività

È possibile trovare la **Pianificazione attività** nel menu principale di ESET Cyber Security Pro in **Strumenti**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, come data, ora e profilo di scansione predefiniti utilizzati.



La Pianificazione attività consente di gestire e avviare attività pianificate con le configurazioni e le proprietà predefinite. La configurazione e le proprietà contengono informazioni quali la data e l'ora, oltre ai profili specificati da utilizzare durante l'esecuzione dell'attività.

Per impostazione predefinita, in Pianificazione attività vengono visualizzate le attività pianificate seguenti:

- Manutenzione registro (dopo aver attivato l'opzione **Mostra attività di sistema** nella configurazione della pianificazione attività)
- Controllo file di avvio dopo l'accesso dell'utente
- Controllo file di avvio dopo il completamento dell'aggiornamento del database delle firme antivirali

- Aggiornamento automatico regolare
- Aggiornamento automatico dopo l'accesso dell'utente

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), premere il pulsante ctrl, fare clic sull'attività che si desidera modificare e selezionare **Modifica...** oppure selezionare l'attività e fare clic sul pulsante **Modifica attività...**.

11.2.1 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi attività...** oppure premere il pulsante ctrl, fare clic nel campo vuoto e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione**
- **Aggiornamento**
- **Manutenzione registro**
- **Scansione del computer su richiesta**
- **Controllo del file di avvio del sistema**

Poiché gli aggiornamenti rappresentano le attività pianificate utilizzate con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento.

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività**. Selezionare la frequenza dell'attività dal menu a tendina **Esegui attività**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento.

Selezionando **Definito dall'utente**, verrà richiesto di specificare la data/l'ora in formato cronologico (per ulteriori informazioni, consultare la sezione Creazione di un'attività definita dall'utente 19).

Nella fase successiva, è quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Attendi l'ora pianificata successiva**
- **Esegui l'attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato** (è possibile definire l'intervallo utilizzando l'opzione **Intervallo minimo di attività**)

Nel passaggio successivo viene visualizzata una finestra contenente un riepilogo delle informazioni relative all'attività corrente pianificata. Fare clic sul pulsante **Fine**.

La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

Per impostazione predefinita, il sistema contiene attività pianificate essenziali per garantire il corretto funzionamento del sistema. Poiché tali attività non devono essere modificate, sono nascoste per impostazione predefinita. Per modificare tale opzione e rendere visibili tali attività, accedere alla sezione **Configurazione** > **Immettere preferenze applicazione ...** (oppure premere *cmd-,*) > **Pianificazione attività** e selezionare l'opzione **Mostra attività di sistema**.

11.2.2 Creazione di un'attività definita dall'utente

È necessario inserire la data e l'ora dell'attività **Definita dall'utente** in formato cronologico con l'anno esteso (stringa che comprende 6 campi separati da uno spazio bianco):
`minuto(0-59) ora(0-23) giorno del mese(1-31) mese(1-12) anno(1970-2099) giorno della settimana(0-7) (domenica = 0 o 7)`

Esempio:
`30 6 22 3 2012 4`

Caratteri speciali supportati nelle espressioni cronologiche:
- asterisco (`*`) - l'espressione corrisponderà a tutti i valori del campo, es. l'asterisco nel 3° campo (giorno del mese) indica ogni giorno
- trattino (`-`) - definisce gli intervalli, es. `3-9`
- virgola (`,`) - separa gli elementi di un elenco, es. `1,3,7,8`
- barra (`/`) - definisce gli incrementi degli intervalli, es. `3-28/5` nel 3° campo (giorno del mese) indica il 3° giorno del mese e successivamente ogni 5 giorni.

I nomi dei giorni (Monday-Sunday) e dei mesi (January-December) non sono supportati.

NOTA: Se si definiscono sia il giorno del mese sia il giorno della settimana, il comando verrà eseguito sono in caso di corrispondenza di entrambi i campi.

11.3 Quarantena

Lo scopo principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET Cyber Security Pro.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati ai laboratori ESET delle minacce per l'analisi.

I file salvati nella cartella di quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, aggiunto dall'utente…) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni). La cartella di quarantena contenente i file in quarantena (*/Libreria/Assistenza applicazione/Eset/esets/cache/quarantena*) rimane nel sistema anche in seguito alla disinstallazione ESET Cyber Security Pro. I file in quarantena sono archiviati in un formato sicuro criptato e possono essere ripristinati dopo l'installazione di ESET Cyber Security Pro.

11.3.1 Mettere file in quarantena

ESET Cyber Security Pro mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando il pulsante **Quarantena** . Per questa operazione, è possibile utilizzare anche il menu contestuale: premere il pulsante ctrl, fare clic nel campo vuoto, selezionare **Quarantena**, scegliere il file che si desidera mettere in quarantena e fare clic sul pulsante **Apri**.

11.3.2 Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Per questa operazione, utilizzare il pulsante **Ripristina**. L'operazione di ripristino è anche disponibile dal menu contestuale premendo il pulsante ctrl, facendo clic sul file specificato nella finestra Quarantena, quindi su **Ripristina**. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

11.3.3 Invio di file dalla Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato valutato erroneamente come infetto (ad esempio da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file al Laboratorio delle minacce ESET. Per inviare un file proveniente dalla quarantena, premere il pulsante ctrl, fare clic sul file e selezionare **Invia file per analisi** dal menu contestuale.

11.4 Processi in esecuzione

L'elenco di **Processi in esecuzione** contiene i processi in esecuzione sul computer in uso. ESET Cyber Security Pro fornisce informazioni dettagliate sui processi in esecuzione allo scopo di garantire la protezione degli utenti mediante la tecnologia ESET Live Grid.

- **Processo** - nome del processo attualmente in esecuzione sul computer in uso. Per visualizzare tutti i processi in esecuzione, è anche possibile utilizzare la funzione Monitoraggio attività (in */Applicazioni/Utility*).
- **Livello di rischio** - nella maggior parte dei casi, ESET Cyber Security Pro e la tecnologia ESET Live Grid assegnano livelli di rischio agli oggetti (file, processi e così via) utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto analizzandone il potenziale relativo all'attività dannosa. Agli oggetti viene assegnato un livello di rischio sulla base di queste regole euristiche. Le applicazioni note contrassegnate di verde sono definitivamente pulite (inserite nella whitelist) e saranno escluse dal controllo. Tale operazione migliorerà la velocità sia del controllo su richiesta sia del controllo in tempo reale. Se un'applicazione è contrassegnata come sconosciuta (in giallo), non si tratta necessariamente di software dannoso. In genere, si tratta semplicemente di un'applicazione più recente. Se non si è sicuri del file, è possibile inviarlo per l'analisi al laboratorio ESET preposto allo studio delle minacce. Se si scopre che il file è un'applicazione dannosa, il suo rilevamento verrà aggiunto ad uno degli aggiornamenti successivi.
- **Numero di utenti** - numero di utenti che utilizzano una data applicazione. Queste informazioni vengono raccolte mediante la tecnologia ESET Live Grid.
- **Orario del rilevamento** - periodo di tempo dal rilevamento dell'applicazione da parte della tecnologia ESET Live Grid.
- **ID bundle applicazione** - nome del fornitore o del processo di applicazione.

Facendo clic su un dato processo, appariranno le seguenti informazioni nella parte inferiore della finestra:

- **File** - posizione di un'applicazione nel computer in uso,
- **Dimensioni file** - dimensione fisica del file sul disco,
- **Descrizione file** - caratteristiche del file basate sulla descrizione del sistema operativo,
- **ID bundle applicazione** - nome del fornitore o del processo di applicazione,
- **Versione file** - informazioni provenienti dal pubblicatore dell'applicazione,
- **Nome prodotto** - nome dell'applicazione e/o ragione sociale.

11.5 Live Grid

Il Sistema di allarme immediato Live Grid è uno strumento in grado di informare in modo immediato e costante ESET sulle nuove infiltrazioni. Il sistema di allarme immediato bidirezionale Live Grid è stato concepito con un unico scopo: migliorare la sicurezza degli utenti. Il sistema migliore per garantire il rilevamento di nuove minacce subito dopo la loro comparsa consiste nell'"effettuare il collegamento" al maggior numero possibile di clienti e nell'utilizzo degli stessi come rilevatori di minacce. Esistono due opzioni:

1. Si può decidere di non attivare il sistema di allarme immediato Live Grid. Non verrà persa alcuna funzionalità del software e l'utente continuerà a ricevere il livello migliore di protezione offerto dal sistema.
2. È possibile configurare il sistema di allarme immediato Live Grid per inviare informazioni anonime relative alle nuove minacce e alle posizioni del nuovo codice di minaccia. Questo file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce aiuterà ESET ad aggiornare il suo database di minacce e a migliorare le capacità di rilevamento delle minacce del programma.

Il sistema di allarme immediato Live Grid raccoglierà informazioni sul computer correlate alle nuove minacce rilevate. Queste informazioni possono includere un campione o una copia del file in cui è comparsa la minaccia, il percorso a quel file, il nome del file, la data e l'ora, il processo di comparsa della minaccia sul computer e le informazioni relative al sistema operativo installato sul computer.

Sebbene sia possibile che tale sistema riveli occasionalmente alcune informazioni relative all'utente o al computer in uso (nomi utente in un percorso di directory e così via) al Laboratorio delle minacce ESET, tali informazioni verranno utilizzate ESCLUSIVAMENTE per consentire a ESET di rispondere immediatamente alle nuove minacce.

La configurazione di Live Grid è accessibile da **Configurazione** > **Inserire preferenze applicazione...** (oppure premere *cmd-,*) > **Live Grid**. Selezionare l'opzione **Attiva Sistema di allarme immediato Live Grid** per attivare, quindi fare clic sul pulsante **Configurazione...** vicino all'intestazione **Opzioni avanzate**.

11.5.1 Configurazione Live Grid

Per impostazione predefinita, ESET Cyber Security Pro è configurato in modo da inviare i file sospetti al laboratorio ESET preposto allo studio delle minacce per analisi dettagliate. Se non si desidera inviare questi file automaticamente, deselezionare l'opzione **Invio di file sospetti**.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi al laboratorio ESET preposto allo studio delle minacce. Per eseguire questa operazione, fare clic su **Strumenti** > **Invia file per analisi** dalla finestra principale del programma. In caso di rilevamento di un'applicazione dannosa, questa verrà aggiunta al successivo aggiornamento del database delle firme antivirali.

Invio di informazioni statistiche anonime - Il Sistema di allarme immediato ESET Live Grid raccoglie informazioni in forma anonima sul computer correlate alle minacce rilevate di recente. Queste informazioni comprendono il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione del prodotto di protezione ESET, la versione del sistema operativo in uso e le impostazioni di ubicazione. Le statistiche vengono generalmente inviate ai server ESET una o due volte al giorno.

Segue un esempio di un pacchetto statistico inviato:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463
[1].zip
```

Filtro di esclusione - Questa opzione consente di escludere dall'invio determinati tipi di file. È utile, ad esempio, escludere file che potrebbero contenere informazioni riservate, ovvero documenti o fogli di calcolo. I tipi di file più comuni sono esclusi per impostazione predefinita (.doc, .rtf e così via). È possibile aggiungere qualunque tipologia di file alla lista degli elementi esclusi dal controllo.

Indirizzo e-mail del contatto (facoltativo) - L'indirizzo e-mail dell'utente sarà utilizzato qualora sia necessario ottenere ulteriori informazioni ai fini dell'analisi. Nota: non verrà ricevuta alcuna risposta da ESET eccetto nel caso in cui siano necessarie ulteriori informazioni.

12. Interfaccia utente

Le opzioni di configurazione dell'interfaccia utente consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche. È possibile accedere a tali opzioni dalla sezione **Configurazione** > **Inserire preferenze applicazione...** (oppure premere *cmd-,*) > **Interfaccia**.

Per visualizzare la schermata iniziale ESET Cyber Security Pro all'avvio del sistema, selezionare l'opzione **Mostra schermata iniziale all'avvio**.

L'opzione **Presenta applicazione in dock** consente di visualizzare l'icona ESET Cyber Security Pro nel dock del sistema operativo Mac e di passare da ESET Cyber Security Pro ad altre applicazioni in esecuzione premendo *cmd-tab*. Le modifiche avranno effetto al riavvio di ESET Cyber Security Pro (attivato generalmente dal riavvio del computer).

L'opzione **Utilizza menu standard** consente di utilizzare alcuni tasti di scelta rapida (vedere Tasti di scelta rapida 6) e di visualizzare voci del menu standard (Interfaccia utente, Configurazione e Strumenti) sulla barra dei menu del sistema operativo MAC (nella parte superiore della schermata).

Per attivare le descrizioni dei comandi per alcune opzioni di ESET Cyber Security Pro, selezionare l'opzione **Mostra descrizioni comandi**.

L'opzione **Mostra file nascosti** consente di visualizzare e selezionare i file nascosti nella configurazione **Destinazioni di scansione** di una **Scansione computer**.

12.1 Avvisi e notifiche

La sezione **Avvisi e notifiche** consente di configurare la gestione degli avvisi delle minacce e delle notifiche di sistema in ESET Cyber Security Pro.

La disattivazione dell'opzione **Visualizza avvisi** annullerà tutte le finestre di avviso ed è pertanto adatta solo a situazioni specifiche. Nella maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

La selezione dell'opzione **Visualizza notifiche sul desktop** consentirà di attivare le finestre di avviso che non richiedono l'interazione da parte dell'utente per poterle visualizzare sul desktop (per impostazione predefinita, l'angolo in alto a destra dello schermo). È possibile definire il periodo durante il quale verrà visualizzata una notifica modificando il valore **Chiudi automaticamente notifiche dopo** X **secondi**.

Se si desidera visualizzare solo le notifiche che richiedono l'interazione dell'utente durante l'esecuzione delle applicazioni a schermo intero, selezionare l'opzione **Attiva modalità a schermo intero**. Questa opzione è utile nel caso di presentazioni, giochi o altre attività che richiedono la visualizzazione a schermo intero.

12.1.1 Configurazione avanzata avvisi e notifiche

ESET Cyber Security Pro consente di visualizzare le finestre di dialogo degli avvisi che informano l'utente in merito ad una nuova versione del programma, ad un nuovo aggiornamento del sistema operativo, alla disattivazione di alcuni componenti del programma, all'eliminazione dei rapporti e così via. È possibile rimuovere ciascuna notifica selezionando l'opzione **Non mostrare nuovamente questa finestra di dialogo** in ciascuna finestra di dialogo.

Elenco di finestre di dialogo (**Configurazione** > **Inserire preferenze applicazione...** > **Avvisi e notifiche** > **Configurazione...**) consente di visualizzare l'elenco di tutte le

finestre di dialogo attivate da ESET Cyber Security Pro. Per attivare o rimuovere ciascuna notifica, utilizzare la casella di controllo sulla sinistra di **Nome della notifica**. È possibile inoltre definire le **Condizioni di visualizzazione** in base alle quali verranno visualizzate le notifiche relative ad una nuova versione del programma e all'aggiornamento del sistema operativo.

12.2 Privilegi

Le impostazioni di ESET Cyber Security Pro rivestono un ruolo fondamentale dal punto di vista dei criteri di sicurezza dell'organizzazione di appartenenza. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Di conseguenza, è possibile scegliere quali utenti potranno modificare la configurazione del programma.

Per specificare gli utenti con privilegi, fare clic su **Configurazione** > **Inserire preferenze applicazione...** (oppure premere *cmd-,*) > **Privilegi**.

Per garantire la massima sicurezza del sistema, è necessario configurare correttamente il programma. Qualsiasi modifica non autorizzata può provocare la perdita di dati importanti. Per definire una lista di utenti con privilegi, selezionarli dalla lista **Utenti** sul lato sinistro e fare clic sul pulsante **Aggiungi** . Per visualizzare tutti gli utenti del sistema, selezionare l'opzione **Mostra tutti gli utenti**. Per rimuovere un utente, selezionarne il nome nella lista **Utenti con privilegi** sulla destra e fare clic su **Rimuovi**.

NOTA: Se la lista di utenti con privilegi è vuota, tutti gli utenti del sistema saranno autorizzati a modificare le impostazioni del programma.

12.3 Menu contestuale

È possibile attivare l'integrazione del menu contestuale nella sezione **Configurazione** > **Inserisci preferenze applicazione ...** (oppure premere *cmd-,*) > sezione **Menu contestuale** selezionando l'opzione **Integra nel menu contestuale**. Per rendere effettive le modifiche, è necessario uscire o riavviare il computer. Le opzioni del menu contestuale saranno disponibili nella finestra **Finder** premendo il tasto ctrl e facendo clic su qualsiasi file.

13. Varie

13.1 Importa ed esporta impostazioni

Le configurazioni di importazione e di esportazione di ESET Cyber Security Pro sono disponibili nel pannello **Configurazione**.

Sia l'importazione che l'esportazione utilizzano i file di archivio per memorizzare la configurazione. Le opzioni di importazione e di esportazione sono utili nel caso in cui si desideri effettuare il backup della configurazione corrente di ESET Cyber Security Pro per poterlo utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per quegli utenti che desiderino utilizzare la configurazione preferita di ESET Cyber Security Pro su più sistemi. In tal modo, infatti, sarà possibile importare facilmente il file di configurazione per il trasferimento delle impostazioni desiderate.

13.1.1 Importa impostazioni

Per importare una configurazione, fare clic su **Configurazione** > **Importa ed esporta impostazioni...** dal menu principale, quindi selezionare l'opzione **Importa impostazioni**. Inserire il nome del file di configurazione o fare clic sul pulsante **Sfoglia...** per ricercare il file di configurazione che si desidera importare.

13.1.2 Esporta impostazioni

Per esportare una configurazione, fare clic su **Configurazione** > **Importa ed esporta impostazioni...** dal menu principale. Selezionare l'opzione **Esporta impostazioni** e immettere il nome del file di configurazione. Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.

13.2 Configurazione del server proxy

È possibile configurare le impostazioni del server proxy in **Configurazione** > **Inserire preferenze applicazione...** (oppure premere *cmd-,*) > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per tutte le funzioni di ESET Cyber Security Pro. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy per questo livello, selezionare la casella di controllo **Utilizza server proxy** e inserire l'indirizzo IP o URL del server proxy nel campo **Server proxy**. Nel campo **Porta**, specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128).

Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e immettere **Nome utente** e **Password** validi nei rispettivi campi.

14. Glossario

14.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

14.1.1 Virus

Un virus è un'infiltrazione che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili, gli script e i documenti. Per replicarsi, un virus allega il suo "corpo" alla fine di un file di destinazione. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché dispongono della capacità di eliminare di proposito i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante tenere presente che i virus (se paragonati a trojan o spyware) sono sempre più rari, poiché non sono commercialmente allettanti per gli autori di software dannosi. Inoltre, il termine "virus" è spesso utilizzato in modo errato per indicare tutti i tipi di infiltrazioni. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare lo stato originale dei file infetti, ovvero pulirli utilizzando un programma antivirus.

14.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, essi possono espandersi in tutto il mondo entro poche ore dal rilascio e, in taluni casi, perfino entro pochi minuti. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

14.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Oggigiorno, tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "Trojan horse" ("cavallo di Troia") ha assunto un'accezione molto generale che indica un'infiltrazione che non rientra in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- Downloader: un programma dannoso in grado di scaricare altre infiltrazioni da Internet.
- Dropper: un tipo di trojan horse concepito per installare sui computer compromessi altri tipi di malware.
- Backdoor: un'applicazione che comunica con gli aggressori remoti, consentendo loro di ottenere l'accesso a un sistema e prenderne il controllo.
- Keylogger (registratore delle battute dei tasti): un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli aggressori remoti.
- Dialer - i dialer sono programmi progettati per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti la creazione di una nuova connessione. I dialer possono causare danni solo agli utenti che dispongono di una connessione remota, utilizzata oramai sempre più di rado.
- Solitamente, i Trojan horse assumono la forma di file eseguibili. Se sul computer in uso viene rilevato un file classificato come Trojan horse, si consiglia di eliminarlo, poiché contiene probabilmente un codice dannoso.

14.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli aggressori di Internet l'accesso illimitato ad un sistema, nascondendo al contempo la loro presenza. I rootkit, dopo aver effettuato l'accesso ad un sistema (generalmente sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per evitare il rilevamento da parte del software antivirus: nascondono i processi e i file. Per questo motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per la prevenzione dei rootkit, esistono due livelli di rilevamento:

1. Quando tentano di accedere ad un sistema. Non sono ancora presenti e sono pertanto inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2. Quando sono nascosti al normale testing.

14.1.5 Adware

Adware è l'abbreviazione di software supportato dalla pubblicità ("advertising-supported software"). Rientrano in questa categoria i programmi che consentono di visualizzare materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono agli sviluppatori di freeware di coprire i costi di sviluppo delle proprie applicazioni (in genere utili).

L'adware di per sé non è pericoloso, ma gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento, allo stesso modo dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

14.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/la consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware spesso sono associati a versioni gratuite di un programma dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire il passaggio a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

14.1.7 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET Cyber Security Pro offre la possibilità di rilevare tali minacce.

"Applicazioni potenzialmente pericolose" è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente), si prega di rivolgersi all'amministratore di rete o di rimuovere l'applicazione.

14.1.8 Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- apertura di nuove finestre mai viste in precedenza
- attivazione ed esecuzione di processi nascosti
- maggiore utilizzo delle risorse del sistema
- modifiche dei risultati di ricerca
- applicazioni che comunicano con server remoti.

14.2 Tipi di attacchi remoti

Esistono molte tecniche particolari che consentono agli aggressori di compromettere i sistemi remoti. Tali tecniche sono suddivise in varie categorie.

14.2.1 Attacchi DoS

DoS, acronimo di Denial of Service, ovvero negazione del servizio, è un tentativo di rendere un computer o una rete non disponibile per gli utenti potenziali. Le comunicazioni tra gli utenti colpiti da tali attacchi vengono bloccate e non possono più continuare in modo funzionale. Per un funzionamento corretto, i computer esposti ad attacchi DoS devono essere generalmente riavviati.

Nella maggior parte dei casi, le destinazioni preferite sono i server web e l'obiettivo consiste nel renderli non disponibili agli utenti per un determinato periodo di tempo.

14.2.2 DNS Poisoning

Mediante il metodo di DNS poisoning (Domain Name Server), gli hacker possono ingannare il server DNS di qualsiasi computer facendo credere che i dati fasulli forniti siano legittimi e autentici. Le informazioni fasulle vengono memorizzate nella cache per un determinato periodo di tempo, consentendo agli aggressori di riscrivere le risposte DNS per gli indirizzi IP. Di conseguenza, gli utenti che tentano di accedere a siti web su Internet scaricheranno nel computer virus o worm, invece dei contenuti originali.

14.2.3 Attacchi worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. I worm di rete sfruttano le vulnerabilità di diverse applicazioni. Grazie alla disponibilità di Internet, possono diffondersi in tutto il mondo entro poche ore dal loro rilascio e, in alcuni casi, persino entro pochi minuti.

La maggior parte degli attacchi worm (Sasser, SqlSlammer) può essere evitata utilizzando le impostazioni di protezione predefinite del firewall, oppure bloccando le porte non protette e inutilizzate. Inoltre, è fondamentale aggiornare il sistema operativo in uso installando le patch di sicurezza più recenti.

14.2.4 Controllo delle porte

Il controllo delle porte consente di individuare le porte del computer aperte su un host di rete. Uno scanner di porte è un software progettato per rilevare tali porte.

La porta di un computer è un punto virtuale che gestisce i dati in entrata e in uscita: un elemento cruciale dal punto di vista della sicurezza. In una rete di grandi dimensioni, le informazioni raccolte dagli scanner delle porte possono aiutare l'utente a identificare potenziali vulnerabilità. Tale uso è legittimo.

Tuttavia, il controllo delle porte viene spesso utilizzato dagli hacker nel tentativo di compromettere la sicurezza. Il primo passo consiste nell'invio di pacchetti a ogni porta. In base al tipo di risposta, è possibile stabilire quali sono le porte in uso. Il controllo in sé non causa danni, ma occorre tener presente che questa attività può rivelare potenziali vulnerabilità e consente agli aggressori di prendere il controllo dei computer remoti.

Si consiglia agli amministratori di rete di bloccare tutte le porte inutilizzate e di proteggere quelle in uso dagli accessi non autorizzati.

14.2.5 Desincronizzazione del TCP

La desincronizzazione del TCP è una tecnica utilizzata negli attacchi Hijacking TCP. È avviata da un processo in cui il numero sequenziale dei pacchetti in entrata è diverso dal numero sequenziale atteso. I pacchetti con un numero sequenziale inatteso vengono ignorati (o salvati nella memoria buffer, se sono presenti nella finestra della comunicazione corrente).

Nello stato di desincronizzazione, entrambi gli endpoint della comunicazione ignorano i pacchetti ricevuti. In questa fase, gli aggressori remoti sono in grado di infiltrarsi e di fornire pacchetti con un numero sequenziale corretto. Gli aggressori sono persino in grado di manipolare o di modificare la comunicazione.

Gli attacchi Hijacking mirano all'interruzione delle comunicazioni server-client o peer-to-peer. Molti attacchi possono essere evitati utilizzando l'autenticazione per ciascun segmento TCP. Si suggerisce inoltre di utilizzare le configurazioni consigliate per i dispositivi di rete in uso.

14.2.6 SMB Relay

SMBRelay e SMBRelay2 sono programmi particolari in grado di attaccare computer remoti. Questi programmi si avvalgono del protocollo di condivisione file Server Message Block sovrapposto su NetBIOS. Se un utente condivide una cartella o una directory all'interno della LAN, utilizza molto probabilmente questo protocollo di condivisione file.

Nell'ambito della comunicazione della rete locale, vengono scambiate password hash.

SMBRelay riceve una connessione sulle porte UDP 139 e 445, inoltra i pacchetti scambiati dal client e dal server e li modifica. Dopo aver eseguito la connessione e l'autenticazione, il client

viene disconnesso. SMBRelay crea un nuovo indirizzo IP virtuale. SMBRelay inoltra la comunicazione del protocollo SMB eccetto per la negoziazione e l'autenticazione. Gli aggressori remoti possono utilizzare l'indirizzo IP a condizione che il computer client sia connesso.

SMBRelay2 funziona in base agli stessi principi di SMBRelay, eccetto per il fatto che utilizza i nomi NetBIOS invece degli indirizzi IP. Entrambi sono in grado di eseguire attacchi di tipo "man-in-the-middle". Questi attacchi consentono agli aggressori remoti di leggere, inserire e modificare i messaggi scambiati tra due endpoint di comunicazione senza essere notati. I computer esposti a tali attacchi spesso non rispondono più o si riavviano inaspettatamente.

Per evitare gli attacchi, si consiglia di utilizzare password o chiavi di autenticazione.

14.2.7 Attacchi ICMP

ICMP (Internet Control Message Protocol) è un protocollo Internet molto diffuso e ampiamente utilizzato. Viene utilizzato principalmente dai computer in rete per inviare diversi messaggi di errore.

Gli aggressori remoti tentano di sfruttare i punti deboli del protocollo ICMP. Il protocollo ICMP è stato progettato per la comunicazione unidirezionale che non richiede l'autenticazione. Questo consente agli aggressori remoti di attivare i cosiddetti attacchi DoS (Denial of Service, negazione del servizio) o gli attacchi che consentono a soggetti non autorizzati di accedere ai pacchetti in ingresso e in uscita.

Esempi tipici di attacchi ICMP includono attacchi ping flood, ICMP_ECHO flood e smurf. I computer esposti ad attacchi ICMP risultano notevolmente più lenti (ciò riguarda tutte le applicazioni che utilizzano Internet) e presentano problemi di connessione a Internet.

14.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi È un servizio flessibile, rapido e diretto che ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa del loro elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Tra gli esempi tipici di messaggi di spam figurano annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli per gli utenti è il fatto che i costi di invio dei messaggi di spam sono minimi e gli autori di messaggi di spam dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Inoltre, il volume e la varietà dei messaggi di spam ne rende estremamente difficoltoso il controllo. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spam. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet,
- fornire il proprio indirizzo e-mail solo a utenti attendibili,
- se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati,
- non rispondere a messaggi di spam già recapitati nella posta in arrivo,
- quando si compilano moduli su Internet, prestare particolare attenzione a opzioni del tipo *Sì, desidero ricevere informazioni su...*
- utilizzare indirizzi e-mail "specializzati", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via.
- cambiare di tanto in tanto l'indirizzo e-mail,
- utilizzare una soluzione antispam.

14.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggiore crescita. I vantaggi principali dal punto di vista del marketing sono i costi minimi e un livello elevato di immediatezza. Inoltre, i messaggi vengono recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché un utente può essere interessato a ricevere informazioni commerciali su determinati prodotti. Tuttavia, numerose società inviano messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema che non mostra segni di flessione. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi di spam come messaggi legittimi.

14.3.2 Hoax

Un hoax è un messaggio disinformativo diffuso su Internet che viene generalmente inviato via e-mail oppure tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è spesso una burla o una leggenda metropolitana.

Gli hoax di virus dei computer tentano di generare paura, incertezza e dubbio (FUD, Fear, Uncertainty and Doubt) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax chiedono ai destinatari di inoltrare i messaggi a tutti i contatti, perpetuando il ciclo di vita dell'hoax. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Nella maggior parte dei casi è impossibile comprendere le intenzioni dell'autore del messaggio.

Se si riceve un messaggio che invita a inoltrarlo a tutti i contatti, potrebbe trattarsi, con molta probabilità, di un hoax. Su Internet sono presenti molti siti web in grado di verificare l'autenticità di un messaggio e-mail. Se si ritiene che si tratti di hoax, prima di eseguire l'inoltro, effettuare una ricerca su Internet del messaggio.

14.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti allo scopo di ottenere informazioni riservate). Lo scopo consiste nell'ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene eseguito tramite l'invio di messaggi e-mail che assumono le sembianze di quelli di una persona o di una società affidabile (ad es. istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che potrebbero provenire dalla fonte originaria imitata dal messaggio stesso. Con tali messaggi si chiede all'utente, con vari pretesti (verifica di dati, operazioni finanziarie), di inviare alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere facilmente rubati e utilizzati in modo fraudolento.

Le banche, le compagnie di assicurazioni e altre società legittime non chiedono mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

14.3.4 Riconoscimento di messaggi spam

Generalmente, esistono alcuni indicatori che aiutano l'utente a identificare i messaggi spam (e-mail non desiderate) nella casella di posta. Un messaggio può essere considerato un messaggio spam se soddisfa almeno alcuni dei criteri riportati di seguito.

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti,
- agli utenti viene offerta una grossa somma di denaro, a fronte, tuttavia, del versamento di una piccola somma di denaro,
- viene chiesto di immettere, con vari pretesti (verifica di dati, operazioni finanziarie), alcuni dati personali, quali numeri di conti bancari, nomi utente, password e così via.
- è scritto in una lingua straniera,
- viene chiesto di acquistare un prodotto a cui non si è interessati. Se si decide di acquistarlo comunque, si prega di verificare che il mittente del messaggio sia un fornitore attendibile (consultare il produttore originale).
- alcune parole contengono errori di ortografia nel tentativo di aggirare il filtro di spam. Ad esempio *vaigra* invece di *viagra* e così via.